SIMMONS HANLY CONROY, LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
Nicole Ramirez Jones, State Bar No. 279017
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
koncius@kiesel.law
ramirezjones@kiesel.law

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (admitted *pro hac vice*)
230 Park Avenue, 24th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 233-6334
jguglielmo@scott-scott.com

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol, State Bar. No. 194857
Melissa Gardner, State Bar No. 289096
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
msobol@lchb.com
mgardner@lchb.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Douglas Cuthbertson (admitted *pro hac vice*)
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: (212) 355-950
Facsimile: (212) 355-9592
dcuthbertson@lchb.com

Attorneys for Plaintiffs and the Proposed Class
Additional Counsel Listed on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOHN DOE, *et al.*, individually and on behalf of all others similarly situated,

Plaintiffs,

GOOGLE LLC,

Defendant.

This document applies to: All Actions

Case No. 3:23-cv-02431-VC

PLAINTIFFS' RESPONSE TO REQUEST FOR SUPPLEMENTAL BRIEFING RE GOOGLE'S MOTION TO DISMISS SECOND AMENDED CONSOLIDATED COMPLAINT

Judge: Hon. Vince Chhabria
Ctrm: 4, 17th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

Statutes

I. INTRODUCTION

The Court's March 20, 2025 Order, Dkt. No. 191 ("Order"), requested further briefing on four issues related to Google's Motion to Dismiss the Second Amended Complaint.

First, the Court explains the difficulty it has encountered in applying concepts of intent from the Electronic Communications Privacy Act (ECPA) and the California Invasion of Privacy Act (CIPA), which it perceives to arise from a lack of clear overlap between the statutes and Plaintiffs' claims. Dkt. 191 at 1. The Court tentatively reasons that could be addressed by focusing the *mens rea* requirements on the subject matter of communications at issue in the lawsuit. *Id.* at 4. Plaintiffs respond to this aspect of the Court's analysis by explaining why there is no need to re-focus the intent analysis from the concept of intent codified in the statutes, which looks only at whether Google intended to intercept the content of their communications, not what that content is. Plaintiffs provide the legal authority and support for their position.

Second, the Court discusses its understanding of how the technology at issue (the "Google Source Code") allegedly works, including how data it transmits to Google can be used to identify Class members. *Id.* at 2-4. Plaintiffs seek to correct certain minor misunderstandings of their allegations in the Order, and then explain how "identifiability" fits into Plaintiffs' theory of the claims addressed in the Order. Plaintiffs also respond to the Court's question regarding the identifiability of individuals who do not have Google Accounts by identifying allegations as requested and other reasons to permit claims for those Class members to proceed to discovery.

Third, following its conclusions that Plaintiffs sufficiently allege Google's ability to link health information to Google Account holders, the Court indicates that Plaintiffs (all of whom are Google Account holders) likely also sufficiently plead a breach of contract claim. Plaintiffs agree with this conclusion, and respond to Google's counter-arguments by explaining why they are unsupported, not only by any allegation or deficiency in the SAC, but also by authority.

Fourth, applying the intent analysis described at the outset of its Order, the Court tentatively concludes that Plaintiffs adequately allege Google intended to intercept their health information, at least prior to March 2023. After March 2023, the Court tentatively finds that a Help

Page entitled "HIPAA and Google Analytics" (Dkt. 165-3) makes it unreasonable to "infer … that Google intended to receive personal health information that could be linked to identifiable Google account holders" for two reasons: (1) this "disclosure…told providers not to use Google's products on any page that may be related to the provision of health care services"; and (2) "this would prevent the gid cookie from sending personal health information in a way that would allow Google to link it to identifiable Google account holders." Dkt. 191 at 5.

Plaintiffs agree with the Court's conclusions as to Google's pre-March 2023 conduct. With respect to the Court's post-March 2023 analysis, Plaintiffs explain why: (1) their allegations are sufficient to establish intent, and (2) Google's Help Page does not require dismissal of claims involving Google's post-March 2023 conduct, no matter what standard the Court applies.

II. ARGUMENT

A. This Case Fits the ECPA and CIPA Intent Analysis.

Plaintiffs agree with the Court that the SAC adequately pleads Google's intent to intercept private health information that Google can link to a particular, identifiable individual. *See* Dkt. 191 at 4. Plaintiffs disagree with the standard that the Court applies to reach its correct conclusion, because applicable law does not require proof of Google's intent to acquire health information *per se*, but rather that Google had the intent to "intercept" the contents of communications.

The analysis concerning Google's intent under the law remains the same here as in all cases alleging unlawful interception or recording of communications, namely: "the operative question . . . is whether the defendant acted consciously and deliberately with the goal of intercepting wire communications." *United States v. Christensen*, 828 F.3d 763, 775 (9th Cir. 2015). "Intercept" means "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). "Contents" of a communication "includes any information concerning the substance, purport, or meaning of that communication." *Id.* §2510(8). Therefore, Plaintiffs' allegations that Google deploys Google Source Code across the Internet in a manner that, by Google's design, inescapably acquires content of communications (*i.e.*, "any information concerning the substance, purport, or meaning" of

communications) without discriminating as to its subject matter (SAC ¶¶ 85-87, 145, 149, 166), is sufficient to plausibly allege intent within the meaning of applicable statutes.

To be sure, whether this specific content also constitutes "Health Information" relates to other aspects of the case, such as Plaintiffs' breach of contract claim, which turns on specific promises Google made about its collection of health data. *See* Section C, below. But Congressional intent in establishing the concept of intent for the ECPA, as applied in well-reasoned opinions from several appellate courts applying the ECPA (and CIPA), demonstrate that the subject matter and identifiability of Plaintiffs' intercepted communications should not impact the Court's analysis concerning whether Google acted consciously and deliberately in intercepting the "contents" of communications.

1. The ECPA and CIPA § 631 Do Not Support a Subject-Focused Concept of Intent.

A focus on what intercepted communications were about, and what Google might be able to do with them, is inconsistent with the statutory purpose of the ECPA, which CIPA mirrors in California. The state and federal legislature protected privacy in methods of communication because victims of non-consensual surveillance suffer a privacy violation no matter what (if anything) the defendant sought to learn by surveilling them. For this reason, the intent requirements of these statutes focus on whether the interceptions were "deliberate" and "conscious," no matter the content of the communication. *See Christensen*, 828 F.3d at 775.

Legislative history supports this interpretation. In explaining what it means in the ECPA that "the crime of interception . . . consists of the intentional acquisition of the contents of a wire, electronic or oral, communication," the 1986 Report of the Senate Committee on the Judiciary confirms that the focus, initially, is on whether the defendant was deliberately engaged in surveillance activities, as opposed to "picking up of the contents of a communication" incidental to different types of activities, such as electronics testing or scanning for public radio programs. S. Rep. No. 99-541, at 24 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3560, 3578.

Case law is in accord. That interceptions are "deliberate" is often clear from the nature of the technology being deployed. *See e.g.*, *United States v. Hugh*, 533 F.3d 910, 912 (8th Cir. 2008)

(distinguishing bounty hunter using wiretap equipment from telephone repairman fixing a phone). Thus, the Ninth Circuit ruled that the jury did not need to ask *whose* communications "Telesleuth" surveillance software was intended to intercept, only whether the defendant's goal in developing, updating, and using that software was to intercept communications. *Christensen*, 828 F.3d at 791. Likewise, the Second Circuit ruled that it was proper to exclude evidence showing what *type of calls* a defendant using wiretap equipment *wanted* to capture ("the harassing phone calls made to him"), because "[a]ll that is relevant is that [the defendant] intentionally intercepted communications between two unknowing and unconsenting individuals." *United States v. Townsend*, 987 F.2d 927, 928 (2d Cir. 1993); *see also United States v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010), as amended (Nov. 29, 2010) (affirming conviction under ECPA even though defendant did not obtain the type of communications he had hoped to obtain by intentionally monitoring supervisor's inbox).

Courts have also held that the intent standard protects potential defendants who, despite using surveillance equipment deliberately, were not "conscious" of particular interceptions. *See e.g.*, *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 743 (4th Cir. 1994) (no intent where "the fact that the microphone was on was the result of a design defect and was not known to anyone"); *see also*, *e.g.*, *In re HIPAA Subpoena*, 961 F.3d 59, 67 (1st Cir. 2020) (no intent without evidence that employer using call-recording system "was even aware of the [at-issue] recordings' existence," and plausibly forgot to stop recording). This standard does not protect defendants who use surveillance technology *and* are aware the relevant interceptions are occurring. In *Abraham v. Cnty. of Greenville, S.C.*, for example, the Fourth Circuit found ample support for intent where a defendant used wiretap equipment *and* the jury "could reasonably conclude that the [defendant] knew" of the relevant interceptions." *Abraham v. Cnty. of Greenville, S.C.*, 237 F.3d 386, 392 (4th Cir. 2001); *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020) ("several courts have rejected a defendant's claim that the interception was inadvertent where the defendant was aware it was occurring").

The Court has previously concluded that Plaintiffs must plead "something more than mere

awareness that an interception might occur," and that is consistent with authority. Dkt. 157 at 7. That "something more" is the intent to engage in communications surveillance which distinguishes Google from individuals whose "picking up of the contents" of communications was only incidental to other goals, even if they were aware it might occur. S. REP. 99-541, *supra*. Pleading that Google had "the goal to collect 'communications about private health information that Google can link to a particular, identifiable individual,'" (Dkt. 194 at 14), as Plaintiffs have done in the SAC, is sufficient but far more than required to adequately allege Google's intent.

2. CIPA § 632 Does Not Support a Subject-Focused Concept of Intent.

CIPA § 632 imposes the same general pleading requirements for intent. Cal. Penal Code § 632(a) ("[a] person who intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication.").

The Court tentatively reasons that CIPA § 632 requires a subject-focused intent to capture "Health Information" here because the statute protects only "confidential" communications. Dkt. 191 at 4 n.1. This incorrectly equates the subject matter to the "circumstances" in which a communication occurs. "Confidential communication" means "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto." Cal. Penal Code § 632(c). The California Supreme Court has explained that "confidential" does not turn on the communication's contents. *See Flanagan v. Flanagan*, 27 Cal. 4th 766, 774 (2002) ("the phrase 'confined to the parties' in the first clause of subdivision (c) is interpreted to refer to the actual conversation, not its content").

Like the ECPA, non-parties that overhear protected ("confidential") communications by accident, whether in the course of non-surveillance activities, or unconsciously, do not have intent under CIPA § 632. *See People v. Buchanan*, 26 Cal. App. 3d 274, 281, 288 (1972) (finding no intent for a telephone switchboard operator who "inadvertently" overheard a telephone conversation during the "moment[ ]" she was required to stay on the line to ensure a proper connection); *Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 435-36 (2018); *see also*, *e.g.*,

People v. Superior Ct. of Los Angeles Cnty., 70 Cal. 2d 123, 133 (1969) ("[A] person might intend to record the calls of wild birds on a game reserve and at the same time accidentally pick up the confidential discussions of two poachers. To hold the birdwatcher punishable under the statute for such a fortuitous recording would be absurd"). Rather, intent is demonstrated by a "purpose" of surveilling communications in the relevant circumstances, or use of "recording equipment" with knowledge of actual interceptions in the relevant circumstances. *See Rojas*, 20 Cal. App. 5th at 435 (2018) ("[T]he recording of a confidential conversation is intentional if the person using the recording equipment does so with the purpose or desire of recording a confidential conversation, or with the knowledge to a substantial certainty that his use of the equipment will result in the recordation of a confidential conversation.") (citations omitted).

The *Rojas* decision is instructive because it applied the California law to arguments, similar to Google's, that intent requires targeting specific types of communications, or people, and that policies associated with the deliberate use of surveillance equipment negate intent even if they do not negate awareness. *See id.* ("*Rojas I*"); *Rojas v. HSBC Card Servs. Inc.*, 93 Cal. App. 5th 860 (2023), review denied (Nov. 21, 2023) (*Rojas II*).

In *Rojas*, the Defendant (HSBC) used a telephone call recording system that activated automatically when any HSBC customer service employee placed a call from the phone at their desk. The Plaintiff (Rojas) received 317 personal calls from affected HSBC phones while the recording system was in use, primarily because her daughter worked for HSBC as a call center agent. After discovering that HSBC recorded her calls, Rojas alleged that the calls were "confidential" under CIPA § 632 and 632.7, and that HSBC recorded them intentionally. HSBC successfully moved for summary judgment, arguing that it only *intended* to record work-related calls, and "the mere act of HSBC installing a recording device on company phones and 'by chance' recording non-work related calls between [Rojas] and [her d]aughter does not satisfy the 'intentional' requirement of [s]ections 632 and 632.7." *Rojas I*, 20 Cal. App. 5th at 434. The Court of Appeal reversed, remanding for trial with guidance that "there is nothing inadvertent or momentary about HSBC recording the 317 telephone calls at issue here; HSBC was *purposefully*

recording *all* of the calls on the telephone lines from which the 317 communications at issue were recorded." *Id.* at 436.

At trial, HSBC relied on workplace policies prohibiting call center agents from making personal calls at their desks. *Rojas II*, 93 Cal. App. 5th at 865–66; 868-69, 874-75. HSBC also relied on policies notifying employees that personal calls may be recorded, and policies requiring employees to notify others that their calls may be recorded. It testified that "calls were recorded for 'quality purposes'" rather than to obtain "confidential" communications. *Id.* at 874. Despite various policies and testimony indicating that the type of communications HSBC *hoped* to record, and *meant* to record, were business-related, the Court of Appeal found "there was no substantial evidence" HSBC lacked the relevant intent when it also recorded personal ("confidential") calls:

> HSBC's trial theory was that because its workplace policies banned personal calls, it did not intend to record those calls. This theory rests on the premise that the ban worked, such that HSBC did not know personal calls were being made and thus recorded. The trial court accepted HSBC's theory, finding Rojas failed to prove intent because HSBC barred agents from making personal calls at their desks and the calls at issue were "made ... without HSBC's knowledge." The court also disagreed HSBC knew confidential calls were being recorded, citing its recording disclosures and reasonable privacy expectations. But the record negates HSBC's theory, and the court's findings. Not only did HSBC policies not prevent personal calls, but HSBC managers knew they were happening and [Rojas's daughter's] manager even permitted them. These facts, coupled with HSBC's full-time recording system, meant HSBC knew personal calls were being recorded—including any such calls that were confidential . . . . [T]o the extent HSBC had a policy barring personal calls from agents' desk phones, that does not establish such calls actually were prevented—particularly in the absence of a single, clear policy governing personal calls and uniform enforcement of those policies. . . . Rojas therefore met her burden of proof on intent, and there was no substantial evidence for the trial court's findings to the contrary.

Id. at 877.

Rojas I and II illustrate why "some measure" to prevent particular kinds of interceptions (*e.g.*, updating a Help Page) is insufficient to negate allegations of intent, if, as alleged here, the defendant used surveillance equipment by design, and was aware the relevant interceptions were occurring. Google avoids citing authority in its supplemental brief, but none of Google's

previously-cited authority, including *Lozano v. City of Los Angeles*, is to the contrary. *See Lozano v. City of Los Angeles*, 73 Cal. App. 5th 711, 727-28 (2022) (alleged interceptor had no reason to know its in-vehicle recording system was turned on). Plaintiffs address the Court's specific question as to the time period after March 2023 in Section D below.

B. All Content Transmitted Via Google Source Code Is Identifiable, Which Supports But Is Not Dispositive of Plaintiffs' Claims.

Plaintiffs generally agree with the Court that the SAC alleges claims based on Google's interception of "private health information that can be linked to an identifiable person," Dkt. 191 at 1, but the Order suggests inconsistencies between the Court's understanding of the allegations, and the facts and theories of liability that Plaintiffs intended to present. Plaintiffs discuss aspects of the allegations that the Order may misunderstand and/or that Google mischaracterizes below.

1. The Order May Misunderstand Some Aspects of the Allegations.

First, while it is correct that Health Care Providers decide which Google products they would like on their webpages, and which webpages should be affected (Dkt. 191 at 2), Health Care Providers cannot "configure" Google Source Code in any way that prevents it from collecting URLs and other contents of communications where it is embedded (SAC ¶ 85). Nor can Health Care Providers in any way render the data collected un-identifiable. SAC ¶¶ 91-104. It is also alleged that Google encourages Health Care Providers to use Google Source Code, and to place it in the "header" of their web properties so it would operate on every page, throughout every user interaction. SAC ¶¶ 28-29, 114, 122, 146, 169 (explaining "gtm"); Ex. 2 (showing "gtm"). Thus, Google is incorrect to argue the SAC only alleges that interceptions result when Health Care Providers engage in "irresponsible customization in contravention of Google's terms of use," and that Plaintiffs fail to allege unlawful behavior "out of the box." Dkt. 194 at 2, 9, 10. To the contrary, by Google's design, the Google Source Code automatically re-directs identifiable "contents" of communications to Google's servers wherever it is installed. SAC ¶¶ 85-87.[1]

[1] Plaintiffs also dispute Google's characterization of the allegations regarding patient portals. Plaintiffs plainly allege how protected communications were intercepted from patient portal

Second, the Order misunderstands how Plaintiffs describe the relevant "cookies" technology. Cookies are identifiers that are sent in parallel with substantive information about the meaning of the various online communications, *e.g.*, whether the person was making an appointment, paying a bill, or researching a urologist. *See* SAC ¶¶ 24 (cookies enable Google to identify and provide access to, and monitor, particular "audience[s]" for advertising and messages, and cookies enable "tracking" individuals for such purposes because they are transmitted to Google "with other information Google's tracking technologies intercept"); ¶ 91 (at least one identifier is always transmitted); ¶ 93 (listing "classic third-party cookies" identified); ¶¶ 94-98, 269 (discussing "first-party" cookies that consumers cannot block); ¶¶ 99-101 (summarizing identifiers and discussing example). Cookies are not themselves a means of transmission of "content," but, along with other identifiers, track the individual and make the transmissions at issue in this case "identifiable." *See* SAC ¶ 90 (quoting HIPAA); Cal. Civ. Code § 1798.140(aj) (defining unique identifier to include IP address, cookies, and pixel tags). Google characterizes these identifiers as "no more than random strings of numbers" (Dkt. 194 at 5 n.5) but that is true of most well-recognized unique identifiers.

2. The Court Should Find that "Identifiability" Is Alleged for All Class Members.

Turning to the Court's questions about non-Google Account Holders, the SAC alleges that Google commingles personally identifiable information from multiple sources, including information about shipping addresses, precise geo-location, and credit card information connected to a "real" person, with identifiers allegedly transmitted by Google Source Code. *See* SAC ¶ 106. In addition, Google's 2017 Charter for Google Analytics discusses an initiative to "provide Online to Offline measurement at scale" for "store visits" conducted by people in the real world. SAC Ex. 11 at 266, 268. While this kind of linkage, independent of the Google Account, certainly ties the identifiers to real-world identities, Plaintiffs did not plead that connection expressly because such information need not immediately identify a person in the real world to be "identifiable" under the

logins and inside portals. *See e.g.*, SAC ¶¶ 40, 60, 112 ("mychart"), 48 ("sign-on" and in-portal interception); 54, 60, 115 (Cerner); 67 (Epic); SAC Ex. 4 at 2-3 ("patient record pages").

relevant statutes, or to fulfill Plaintiffs' purposes for alleging identifiers. *See* Dkt. 191 at 3.

The import of Plaintiffs' allegations about cookies, and identifiability broadly, is that they render the transmissions by Google Source Code "Health Information" subject to even greater statutory and state common law protections. *See* SAC ¶¶ 90, 112. Under HIPAA, which Health Care Providers presumably try to comply with, the "identifiability" question is whether the data contains characteristics—such as device information, browser settings, unique values, or IP addresses—from which an "anticipated recipient" (here, Google) *could* identify an individual, either using that data in isolation or in combination with other "reasonably available information." SAC ¶ 90. Accordingly, the "identifiability" of data received through Google Source Code does not turn on a single data field or cookie value, such as the gid or cid identifiers, or whether Google actually used identifiable data to make an identification. *See id.*

The allegations about identifiers which invoke HIPAA's protections undermine Google's defenses, as well as supporting Plaintiffs' claims. They make it implausible that Health Care Providers knowingly consented to the interceptions alleged. SAC ¶¶ 221, 223. The identifiability of this information also supports the allegation that, if Health Care Providers did consent, the transmissions via Google Source Code from sensitive pages on their web properties constitutes a crime or tort that triggers 18 U.S.C. § 2511(2)(d); SAC ¶¶ 220, 222, 224. Google's 2018 HIPAA disclaimer—which is misleading as to the inherent and unavoidable identifiability of all transmissions via Google Ads, Google Display Ads, and Google Analytics—shows that Google is not the unwitting victim of irresponsible third parties, but instead further supports the inference Google intended to receive Health Information, SAC ¶¶ 152-60.

Plaintiffs' limited references to Google Signals in the SAC do not change this analysis. *See* SAC ¶¶ 97, 105, 132, and 223. Plaintiffs' communications were "identifiable" to Google for purposes relevant to Plaintiffs' theory of liability *before* they were linked to information about offline identity through Google Signals, if they were. *Id.* ¶ 90. The SAC's allegations about Google Signals only confirm that Google necessarily does, in fact, associate the information it receives from any web property using Google Source Code with Google Accounts. Plaintiffs' point is that

if Google only maintained anonymous identifiers for those transmissions, then it would not be possible for Google to offer "Cross Device-eligible remarketing campaigns" which require Google to know that the person who visited a given website using a desktop computer is the same person who uses a particular mobile device. And, of course, it would not be possible to "update" Google Analytics for any given client to allow "Cross Device" remarketing to the subset of Google Accountholders who both use multiple devices and (according to Google) "consented" to Ads Personalization. *See* SAC ¶ 105. Even if Signals did not impact the Plaintiffs directly (there are no allegations or evidence either way), it would not alter the fact that the contents of communications at issue were "identifiable" as relevant to the claims alleged.

The Court should allow the claims of all Class members to proceed because Plaintiffs adequately allege all elements of their claims as applied to all Class members.

C. Plaintiffs' Breach of Contract Cause of Action Is Well Pled.

Plaintiffs agree with the Court that the SAC adequately alleges the transmission of "health information" in violation of Google's promise not to collect it unless users choose to provide it to Google. Dkt. 191 at 3. Plaintiffs will not repeat their arguments in opposition to Google's unreasonable interpretation of its promise here. *See* Dkt. 169 at 20-21.

Plaintiffs add only that Google's assertion that the SAC *still* does not allege it obtained Plaintiffs' "health information," particularly as a reasonable consumer would understand the term, is completely at odds with authority. Indeed, the majority, if not all, of Google's previously-cited support for the proposition undermines its arguments for dismissal.

In its Motion to Dismiss, Google relied on *Kurowski* for the proposition that "IP addresses, cookie identifiers, device identifiers, account numbers, URLs, and browser fingerprints are just metadata and do not constitute IIHI under HIPAA." Dkt. 164 at 23 (quotation marks omitted, citing *Kurowski v. Rush Sys. for Health*, No. 22-5380, 2024 WL 3455020, at *2 (N.D. Ill. July 18, 2024)). However, Google omitted that the order explained that, while an earlier version of the complaint failed to allege IIHI, after amendment, the complaint did allege IIHI. *See id.*; *see also Kurowski v. Rush Sys. for Health*, No. 22-5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023). As noted

in Plaintiffs' opposition brief, *Kurowski* also upheld the contract claim in the earlier version of the complaint regardless of whether HIPAA applied. Dkt. 169 at 21.

Google relied on *Hartley* for the proposition that "IP addresses, Facebook IDs, cookie identifiers, device identifiers, account numbers, URLs, and buttons, pages, and tabs that were clicked and viewed do not constitute IIHI under HIPAA." Dkt. 164 at 23, citing *Hartley v. Univ. of Chicago Med. Ctr.*, 2023 WL 7386060, at *2 (N.D. Ill. Nov. 8, 2023). Google omitted that after the plaintiff added "allegations that [were] specific to herself," the "absolute dearth" of which was the reason for the first dismissal, the court found that health information, and HIPAA-protected IIHI specifically, was properly alleged. *Hartley v. Univ. of Chicago Med. Ctr.*, No. 22-5891, 2024 WL 1886909, at *2 (N.D. Ill. Apr. 30, 2024).

Notably, the *Becerra* court also relied on the earlier decisions in *Kurowski* and *Hartley* to support that it was unreasonable for HHS to infer identifiability from IP addresses alone (which the court called "metadata") in the "proscribed combination." *Am. Hosp. Ass'n v. Becerra*, 738 F. Supp. 3d 780, 803 n.7 (N.D. Tex. 2024).

Google relied on *Cousin* for the proposition that "data about plaintiffs' use of the website to research doctors, look for providers, and search for medical specialists was not PHI because nothing about the information relates specifically to plaintiffs' health." Dkt. 164 at 21 (quotation marks omitted, citing *Cousin v. Sharp Healthcare*, No. 22-2040, 2023 WL 4484441, at *3 (S.D. Cal. July 12, 2023)). Google omitted that after amendment, the court found that the plaintiffs alleged their "interactions on Defendant's website, while 'unauthenticated' or publicly facing, plausibly involve PHI." *Cousin v. Sharp Healthcare*, 702 F. Supp. 3d 967, 973 (S.D. Cal. 2023). The *Cousin* orders were subsequently vacated on other grounds. *Cousin v. Sharp Healthcare*, No. 22-2040, 2024 WL 1184702, at *10 (S.D. Cal. Mar. 19, 2024).

Google relied on *Jones* for the proposition that "IP address, device used to connect to website, web browser used, date and time of communication, [and] words used to prompt the chat was 'record' information, not content." Dkt. 164 at 19 (quotation marks omitted, citing *Jones v. Peloton Interactive, Inc.*, No. 23-1082, 2024 WL 1123237, at *4 (S.D. Cal. Mar. 12, 2024). Google

omitted that after amendment, the court found the plaintiffs alleged the "software surreptitiously intercepts the data entered by Peloton's customers," and had stated CIPA claims. *Jones v. Peloton Interactive, Inc.*, No. 23-1082, 2024 WL 3315989, at *4 (S.D. Cal. July 5, 2024).

Similarly, Google relied on *Hubbard* for the proposition that "the collection of searches run, videos watched, views and interactions with content and ads, voice and audio information, purchase activity, people with whom a user communicated, browsing history, activity on third-party sites and apps that used Google services, GPS, device sensor data, data from devices located near a user, and advertising ID did not rise to the level of a highly offensive intrusion." Dkt. 170 at 12 (quotation marks omitted), citing *Hubbard v. Google LLC*, No. 19-07016, 2024 WL 3302066, at *2, *7–8 (N.D. Cal. July 1, 2024). Recently, the court found that in their amended complaint, "Plaintiffs sufficiently allege[d] that Google engaged in highly offensive conduct." *Hubbard v. Google LLC*, No. 19-07016, 2025 WL 82211, at *5 (N.D. Cal. Jan. 13, 2025).

Here, as in the cases that Google has relied on, the Court should reject any argument that Plaintiffs *cannot* allege Google Source Code plausibly transmits their "health information," and find that now, after amendment, they have plausibly done so.

D. The 2023 HIPAA Admonition Does Not Prove Google's Lack of Deliberation, Consciousness, or Desire.

The Court reasons that the HIPAA Admonition Help Page Google posted in or around March of 2023 makes it unreasonable to infer from the SAC that Google had the requisite intent, and invited Plaintiffs to identify any errors in the Court's analysis.

The primary reason that the Court is mistaken as to the conduct after March 2023 is that it applies the incorrect standard. Under the standard adopted by Circuit and California Appellate courts discussed above, intent is alleged here because the SAC strongly supports that Google acted with the goal of intercepting communications. Unlike the inadvertent telephone repairman, birdwatcher, or switchboard operator, Google's interceptions were the "natural consequences" of its actions in deploying Google Source Code where, and how, it did. *See Stumm v. Town of Pittsboro*, 355 F. Supp. 3d 751, 763 (S.D. Ind. 2018) (jury could find intent despite defendant's

protestations that its "intent extended only to [certain] conversations").

The Court should also infer from the SAC that Google is nothing like defendants who were unaware of the relevant interceptions. Google processed all data transmitted via Google Source Code, with knowledge of the source, to get "minute-fresh" data across thousands of Health Care Provider web properties for *years*. SAC ¶¶ 24-26, 123-144, 153, 167-173, 186; SAC Ex. 11 at 264. Google was still doing it when, in or around May 2023, Plaintiffs captured the transmissions reflected in Exhibits 1 and 2 to the SAC. SAC ¶ 24.[2] Google analogizes itself to "tape-recorder manufacturers" in its supplemental brief, but tape recorder manufacturers would not receive "information concerning the substance, purport, or meaning of [any] communication." *See* Dkt. 194 at 11; 18 U.S.C. 2510(8). In stark contrast to a tape recorder, Google Source Code is designed to give *Google* a "comprehensive view of the entire customer journey" across myriad industries, including healthcare. SAC Ex. 11 at 263-64. This also distinguishes Google from HIPAA-compliant analytics providers that enter Business Associate Agreements precluding self-serving use of data, which Google refuses to do. SAC ¶ 152 n.77. Google's arguments are inconsistent with what Google allegedly does.

Given the facts alleged here, including the long-term and widespread use of Google's surveillance technology on sensitive health-related webpages, a Help Page posted a few months after government authorities responded to the nationwide privacy problem that Google created is not dispositive to overcome Plaintiffs' allegations that that the interceptions were no "accident." *See Christensen*, 828 F.3d 763. Plaintiffs adequately allege Google's intent for all dates on which it has received, and continues to receive, Health Information.

A secondary reason that the Court is incorrect about the 2023 HIPAA Admonition, even under the proposed heightened standard for intent, is that Plaintiffs allege sufficient facts to show that the relevant interceptions did constantly and consistently happen after March 2023. SAC ¶¶ 33-78; Exs. 1-2. A Help Page downloaded by Google's outside counsel is all Google provides to

[2] Google asserts that these exhibits contain inadmissible expert opinion, but they contain no opinions, only facts.

rebut Plaintiffs' express allegations that Google intended to do what it did. Dkt. 165-1 ¶ 3; SAC ¶¶ 145, 161. Google has offered nothing to establish that it ever notified a single Health Care Provider of the HIPAA Admonition after it was posted. There are a *lot* of Google Help Pages, and it is not a reasonable inference that by simply posting a new one, Google expected it to be found. To this day, the HIPAA Admonition is not referenced in the Google Analytics Terms of Service. *See* Dkt. 165-2; SAC ¶ 226 (Google "appears to be waiting for all of the several thousand Health Care Providers involved in its conduct to realize that they have misunderstood how Google's services operate . . . ."). Without a showing that Google caused the Help Page to be read—by *all* of Plaintiffs' providers, it is not fair to infer from its mere existence that Google *wanted* Providers to even find it, let alone react to it by removing Google Source Code from sensitive pages. *See Gladstone v. Amazon Web Servs., Inc.*, 739 F. Supp. 3d 846, 860 (W.D. Wash. 2024) (rejecting argument, where technology was "designed for the purpose of recording and analyzing communications," that "a catch-all provision [in a *contract*, not a Help Page] requiring its customers to comply with the law generally is enough" to negate intent).

Perhaps the HIPAA Admonition represents "some" measure Google took to prevent itself from receiving the communications at issue even if Google never affirmatively showed it to anyone, but it cannot be that "any" measure is sufficient to bar actual victims of surveillance from Court, as a matter of law. Both before and after March of 2023, moreover, it simply is not plausible that Google had the same "accident" every day across thousands of healthcare provider websites, without wanting to. Here, as in *Rojas* and many other cases cited above, the court should permit the fact-finder to evaluate Google's claims that its 2023 Admonition, or any other measures, prove it lacked a deliberate and conscious state of mind, or even the desire to obtain Health Information. Under any standard, that question will "turn on disputed questions of fact that need development on a full evidentiary record." *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064 (N.D. Cal. 2023).

III. CONCLUSION

Plaintiffs respectfully request that the Court deny Google's Motion for the reasons set forth in the Order as well as the reasons set forth above.

Dated: April 3, 2025

SIMMONS HANLY CONROY LLC

/s/ Jason 'Jay' Barnes
Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
An Truong (admitted *pro hac vice*)
atruong@simmonsfirm.com
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: 212-784-6400
Fax: 212-213-5949

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (admitted *pro hac vice*)
afiorilla@lowey.com
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez Jones, State Bar No. 279017
ramirezjones@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444
Fax: 310-854-0812

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol, State Bar No. 194857
msobol@lchb.com
Melissa Gardner, State Bar No. 289096
mgardner@lchb.com
Jallé H. Dafa, State Bar No. 290637
jdafa@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel.: 415 956-1000
Fax: 415-956-1008

Douglas Cuthbertson (admitted *pro hac vice*)
dcuthbertson@lchb.com

250 Hudson Street, 8th Floor
New York, NY 10013
Tel.: 212 355-9500
Fax: 212-355-9592

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Hal D. Cunningham, State Bar No. 243048
hcunningham@scott-scott.com
Sean Russell, State Bar No. 308962
srussell@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel.: (619) 233-4565
Fax: (619) 233-0508

Joseph P. Guglielmo (admitted *pro hac vice*)
jguglielmo@scott-scott.com
Ethan Binder (admitted *pro hac vice*)
ebinder@scott-scott.com
230 Park Ave., 17th Floor
New York, NY 10169
Tel.: (212) 223-6444
Fax: (212) 223-6334

Attorneys for Plaintiffs and the Proposed Class

ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I hereby attest that all signatories listed, and on whose behalf the filing is submitted, concur in the filing's content and have authorized the filing.

Dated: April 3, 2025

/s/ Melissa Gardner
Melissa Gardner